

**REMARKS**

Applicants respectfully request reconsideration of the present application in light of the following remarks.

Claims 1-22, 25, 27-34, 36, 40, 41 and 43-46 are pending in the current application. Claims 1, 9, 29 and 40 are in independent form.

Applicants incorporate the Request for Reconsideration dated November 16, 2009, in its entirety herein by reference.

**Claim Rejections – 35 U.S.C. § 103**

Claims 1-22, 25, 27-34, 36, 40-41, and 43-46 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Khidekel (US 2001/0027527, hereinafter “Khidekel”) and further in view of Ballantyne (US 5,867,821, hereinafter “Ballantyne”). Applicants respectfully traverse these rejections.

**Initially, Applicants repeat the arguments of the Request for Reconsideration dated November 16, 2009, in its entirety.** Applicants provide the following arguments in addition to the reasoning of the Request for Reconsideration dated November 16, 2009, for clarification purposes and to address differences between the Office Action and the Office Action dated August 7, 2009.

***Signature***

Neither Khidekel nor Ballantyne, alone or in combination, disclose at least, “performing a security check upon each access operation in order to ascertain the identity of a user; assigning a user signature, identifying the user, on the basis of the performed security check without being viewable by the user; assigning at least one role signature, each role signature being assignable to a plurality of users, on the

basis of the performed security check without being viewable by the user[.]" as recited by claim 1, and similarly recited by claims 9, 29 and 40.

Khidekel discloses authenticating a user based on the user's credentials (Khidekel, paragraph [0029]) or based on digital certificates (Khidekel, paragraph [0030]). Authentication is defined by Khidekel to be, "the process of verifying the identity of a party." Khidekel, paragraph [0003]. Khidekel authenticates the user and stores a time stamped record of the authentication. Khidekel, paragraph [0033]. A secured server is then sent a token based on information such as the user's credentials. If a user attempts to gain access to records, a secure server **validates the token** by comparing "the difference between the current time and the authentication time to a predefined threshold. For example, a hospital might define the threshold as one month." Khidekel, paragraph [0035], emphasis added. A user may continuously access a secured server using a token without any authentication process (no identity check)for a length of time (e.g., one month). Accordingly, Khidekel **does not** perform a security check to ascertain the identity of a user upon each access operation and therefore cannot assign any signature on the basis of the performed security check.

The Examiner alleges on page 2 of the Office Action, that:

Khidekel teaches ... performing a security check upon each access operation in order to ascertain the identity of a user; [see paragraph 0029] "The user can be authenticated based on the user's credentials" [see paragraph 35, wherein upon receiving the token, the secure server validates the token by comparing the difference between the current time and the authentication time to the predefined threshold to make sure a duration of time has not expired. It is clear from this that each access operation must be logged and a security check performed because if each access is not logged, there would be an error in the duration of time since the last access operation that was not logged.

Applicants respectfully disagree. The Examiner appears to interpret Khidekel as comparing a difference between the current time and an undisclosed last logged

access operation. Accordingly, the Examiner asserts that if there is no last logged access operation, there would be an error. The Examiner appears to misunderstand Khidekel. Khidekel compares the difference between the current time and an authentication time. Khidekel authenticates a user, issues a token, and from that point on Khidekel only verifies a time elapsed from the single authentication to the current time based on the token. The elapsed time is compared to a threshold in order to determine the validity of the token. Khidekel, paragraphs [0033]-[0036]. If the elapsed time exceeds the threshold, Khidekel requires a user to again authenticate. *Id.* Accordingly, “the last access operation,” is irrelevant.

Although the Examiner states that, “[i]t is clear that each access operation must be logged and a security check performed[,]” Khidekel specifically discloses in paragraph [0036] that, “[u]se of the threshold **can eliminate the need for the user to authenticate with the server 12 each time he wishes to access information on the secure server 36**. The user can simply authenticate with the server 12 once, and then access secure servers based on that authentication until a particular service requires the user to authenticate with the server 12 again.” Emphasis added.

Applicants note that Khidekel is specifically directed to a method that does **not** require ascertaining an identity of a user each time. Khidekel ascertains the identity of a user only once within a specified timeframe and then only checks the validity of the token. For this reason, Khidekel cannot disclose, at least, “performing a security check upon each access operation in order to ascertain the identity of a user; assigning a user signature, identifying the user, on the basis of the performed security check without being viewable by the user; assigning at least one role signature, each role signature being assignable to a plurality of users, on the basis of the performed

security check without being viewable by the user[.]" as recited by claim 1, and similarly recited by claims 9, 29 and 40.

Ballantyne discloses an identification and authentication process. Ballantyne, col. 8, lines 28-38. No signature is assigned based on the process. Accordingly, Ballantyne cannot repair the deficiency of Khidekel.

### ***Signing Each Access Operation***

Neither Khidekel nor Ballantyne disclose, at least, "signing each access operation to electronic data by specifying the user signature and the at least one role signature[.]" as recited by claim 1, and similarly recited by claims 9, 29 and 40, emphasis added.

Even assuming, ***arguendo***, that Khidekel discloses role and user signatures (which, as noted above, Applicants disagree with), Khidekel does not disclose signing each access operation to electronic data. Khidekel is directed to **authorizing** access to data and only maintains records with respect to authentications (security checks).

The Examiner alleges that Khidekel discloses, in paragraphs "0034-0035[.]" signing each access operation to electronic data by specifying the user signature and the at least one role signature. Office Action, p. 3. The Examiner alleges that the "user signature" equates to a "token" and a "role signature" equates to "business rules[.]" Office Action, pp. 2-3. Accordingly, the Examiner alleges that paragraphs [0034] and [0035] of Khidekel disclose that each access operation is signed to electronic data **by specifying the token and the business rules**.

Paragraph [0034] describes a token and information imbedded in the token. Paragraph [0035] is directed to validation of the token in order to grant access to a secure server. Neither of paragraphs [0034] or [0035] have any relation to the signing

of an access operation or disclose specifying a token and business rules. Applicants note that “business rules” are nowhere disclosed in either of paragraphs [0034] or [0035]. Business rules are first disclosed in paragraph [0039] of Khidekel.

Ballantyne does not disclose assigning a user signature and a role signature. Accordingly, Ballantyne cannot repair the deficiency of Khidekel.

### ***Claim Interpretation***

The failure of Khidekel and Ballantyne to disclose the limitations of claims 1, 9, 29 and 40, result from a basic difference between the disclosure of Khidekel, directed to methods of authorizing access, and claims 1, 9, 29 and 40, directed to signing access operations.

Applicants respectfully submit that the “[c]laims are not to be read in a vacuum, and limitations therein are to be interpreted in light of the specification in giving them their broadest reasonable interpretation[.]” MPEP 2111.01 (II), emphasis added. The words of a claim must be given their “plain meaning.” MPEP 2111.01, emphasis added. The “plain meaning” refers to the ordinary and customary meaning given to the term by those of ordinary skill in the art. The plain meaning must be consistent with Applicants’ specification. MPEP 2111.01(I) and (III).

The Examiner fails to interpret the words of the claims according to their plain meaning. In order to reject claims directed to ‘signatures’ by using disclosure related to ‘access authorization,’ the Examiner interprets the word “signature” to mean both a software “token” and “business rules.” One having ordinary skill in the art understands that software tokens are security devices that are used to authorize access to computer services and that “business rules,” as disclosed by Khidekel, represent access restrictions. Khidekel, paragraphs [0036] and [0039]. Even

assuming, *arguendo*, that a token and business rules could be interpreted to be a “user signature” and a “role signature[.]” respectively (which Applicants do not admit), one having ordinary skill in the art would not interpret the disclosure of an access operation using a token to equate to, “signing each access operation to electronic data by specifying the user signature and the role signature[.]” Khidekel nowhere discloses **signing** any access operation to electronic data using a token and business rules. Accordingly, the Examiner does not appear to give any effect to the limitation “signing[.]”

The fact the Khidekel does not disclose signing access operations is highlighted by the Examiner’s admission that Khidekel does not disclose, “recording each access operation and the user signature and the at least one role signature specified for each access operation[.]” Office Action, p. 3. The Examiner alleges that Khidekel discloses signing each access operation to electronic data by specifying the user signature and the at least one role signature, but then fails to disclose that the specified signatures are used in any way. Applicants respectfully submit that Khidekel does not disclose using specified user and role signatures because Khidekel does not disclose any signing of an access operation to electronic data.

Applicants respectfully request that should the Examiner not allow the present application in the next official action, that the Examiner adhere to the strictures of MPEP 2111.01 in interpreting the words of claims 1-22, 25, 27-34, 36, 40, 41 and 43-46.

### ***Nonobviousness***

For at least the reasons stated in the Request for Reconsideration dated November 16, 2009, and the reasons stated above, even assuming, *arguendo*, that

Khidekel and Ballantyne could be combined (which Applicants do not admit), Khidekel in view of Ballantyne cannot render claim 1 obvious. Claims 9, 29 and 40 are patentable for reasons at least similar to those stated above with respect to claim 1, noting that claims 9, 29 and 40 should be interpreted solely based on the limitations recited therein. Claims 2-8, 10-22, 25, 27, 28, 30-34, 36, 41 and 43-46 are patentable at least by virtue of their dependence on at least one of claims 1, 9, 29 or 40. Withdrawal of the rejections and allowance of each of claims 1-22, 25, 27-34, 36, 40, 41 and 43-46 is respectfully requested.

#### **CONCLUSION**

Accordingly, in view of the Request for Reconsideration dated November 16, 2009, and the above remarks, reconsideration of the objections and rejections and allowance of each of claims 1-22, 25, 27-34, 36, 40, 41 and 43-46 in connection with the present application is earnestly solicited.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicant(s) hereby petition(s) for a three (3) month extension of time for filing a reply to the outstanding Office Action and submit the required \$1110.00 extension fee herewith.

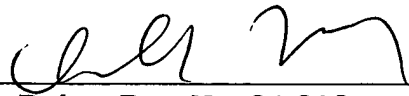
Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Donald J. Daley at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. §1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKY, & PIERCE, P.L.C.

By



Donald J. Daley, Reg. No. 34,313

P.O. Box 8910  
Reston, Virginia 20195  
(703) 668-8000

DJD/AXV:tlt